HKUST – Department of Computer Science and Engineering
COMP170: Discrete Math Tools for CS – Spring 2010

#	LS

Midterm Examination 2

SOLUTION:
Sketch Solution Key

Date: Tuesday , April 20, 2010 Time: 19:00–20:30 Venues: LTA, LTB, LTC

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book exam. It consists of 21 pages and 8 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Only use notation given in class. Do not use notation that you have learnt outside of this class that is nonstandard.
- Calculators may be used for the exam.
- In question 3 and question 4, you are asked for a solution to a recurrence. A *solution* means a formula given in closed form. Formulas using the summation symbol ($\sum$) or ellipses (...) will not be accepted as answers.

Questions	1	2	3	4	5	6	7	8	Total
Points	12	10	14	12	12	12	14	14	100
Score									

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Definitions and Formulas: This page contains some definitions used in this exam and a list of formulas (theorems) that you may use in the exam (without having to provide a proof). Note that you might not need all of these formulas on this exam.

Definitions

1. $N = \{0, 1, 2, 3, \ldots\}$, the set of non-negative integers.
2. $Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers.
3. Z is the set of *all* integers.
4. R is the set of *real numbers*.
5. R^+ is the set of positive *real numbers*.
6. Let $n \in Z^+$. Then $Z_n = \{0, 1, 2, 3, \ldots, (n-2), (n-1)\}$.

Formulas:

1. $\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$
2. If $0 < i < n$ then $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$
3. $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$
4. $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$
5. $p \Rightarrow q$ is equivalent to $\neg p \vee q$
6. $\neg \forall x \in U\,(p(x))$ is equivalent to $\exists x \in U\,(\neg p(x))$
7. $\sum_{i=1}^{n-1} i = n(n-1)/2$
8. $\sum_{i=1}^{n-1} i^2 = \frac{2n^3-3n^2+n}{6}$
9. If $r \neq 1$ then $\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$
10. If $r \neq 1$ then $\sum_{i=0}^{n} ir^i = \frac{nr^{n+2}-(n+1)r^{n+1}+r}{(1-r)^2}$

Student ID: _____

Problem 1: [12 pts]
Find *all* values $n \in Z^+$, such that $3^n > 2^n + 5n^2 - 10$.
Prove the correctness of your answer.

SOLUTION:

The answer is 1 *and all* $n \geq 5$. *Let us check a few of the smallest positive integers:*

$$\begin{aligned}
n = 1: &\quad 3 > -3 = 2 + 5 \cdot 1 - 10 \\
n = 2: &\quad 9 < 14 = 4 + 5 \cdot 4 - 10 \\
n = 3: &\quad 27 < 43 = 8 + 5 \cdot 9 - 10 \\
n = 4: &\quad 81 < 86 = 16 + 5 \cdot 16 - 10 \\
n = 5: &\quad 243 > 147 = 32 + 5 \cdot 25 - 10 \\
n = 6: &\quad 729 > 234 = 64 + 5 \cdot 36 - 10
\end{aligned}$$

We guess that the statement holds for all integers $n \geq 5$. *We prove this by induction on* $n \geq 5$.

Base case: *Already proved above.*

Inductive case: *Let* $n > 5$ *and assume that the statement is true for* $n - 1$, *i.e.,*

$$3^{n-1} > 2^{n-1} + 5(n-1)^2 - 10.$$

This implies that

$$\begin{aligned}
3^n &> 3(2^{n-1} + 5(n-1)^2 - 10) \\
&= 2^n + 2^{n-1} + 15n^2 - 30n + 15 - 30 \\
&= (2^n + 5n^2 - 10) + 2^{n-1} + 10n^2 - 30n - 5
\end{aligned}$$

In order to complete the proof we must now show that, for $n > 5$,

$$2^{n-1} + 10n^2 - 30n - 5 \geq 0.$$

Note that if $n > 5$ *then*

$$10n^2 - 30n = 10n(n-3) > 0$$

and

$$2^{n-1} - 5 \geq 2^4 - 5 > 0$$

so

$$2^{n-1} + 10n^2 - 30n - 5 > 0.$$

This implies that

$$3^n > (2^n + 5n^2 - 10) + 2^{n-1} + 10n^2 - 30n - 5 > 2^n + 5n^2 - 10$$

and we are done.

Student ID: _____

Problem 2: [10 pts]
Construct a contrapositive proof that, for all integers x,

If $(2 + x^2)$ is divisible by 3, then x is not divisible by 3.

SOLUTION:

Let $p(x)$ denote "$(2+x^2)$ is divisible by 3" and $q(x)$ denote "x is not divisible by 3". The statement can be represented as:

$$p(x) \Rightarrow q(x),$$

which is logically equivalent to

$$\neg q(x) \Rightarrow \neg p(x).$$

To construct a contrapositive proof, we first assume that $\neg q(x)$ is true, i.e., x is divisible by 3. Then, $x^2 = 0 \bmod 3$ so $2 + x^2 = 2 \bmod 3$. Then $\neg p(x)$ is correct. Hence the original statement $p(x) \Rightarrow q(x)$ is correct.

Student ID: _____

Problem 3: [14 pts]

Consider a class of n students, each with a distinct student ID number. The TA wants to write down their ID numbers on a paper in increasing order.

If there is only one ID number, i.e., $n = 1$, he just writes down that ID number.

If $n > 1$, he proceeds as follows:

(1) Among all the ID numbers, he first *selects* the largest one.

(2) He writes down the remaining $(n-1)$ ID numbers in increasing order.

(3) He then writes down the largest ID number (found in step (1))

The subtask at Step (2) is solved recursively using the same strategy.

Suppose
- it takes $(n-1)$ seconds to select the largest ID number among n ID numbers and
- it takes 5 seconds to write an ID number on paper.

Let $T(n)$ be the total amount of time in seconds that the TA takes to finish his task.

To start you off we note that $T(1) = 5$ and $T(2) = 11$.

(a) Write a recurrence equation for $T(n)$.
You may assume that $n > 2$.

(b) Give a closed-form solution to $T(n)$. You need to show how you derived your solution.

For both part (a) and part (b) it is not necessary for you to prove the correctness of your solutions.

SOLUTION:

(a) The full recurrence is

$$T(n) = \begin{cases} 5 & \text{if } n = 1 \\ T(n-1) + n + 4 & \text{if } n > 1 \end{cases}$$

You only needed to state this for $n \geq 2$.
The recurrence comes from the fact that,
when processing n items, it takes
(1) $n-1$ seconds to select the larget item
(2) $T(n-1)$ seconds to write down the otehr $n-1$ items in order and
(3) 5 seconds to write the last item.
So,

$$T(n) = (n-1) + T(n-1) + 5 = T(n-1) + n + 4.$$

(b) Iterating the recurrence gives

$$\begin{aligned}
T(n) &= n + 4 + T(n-1) \\
&= (n+4) + (n+3) + T(n-2) \\
&= (n+4) + (n+3) + (n+2) + T(n-3) \\
&= \cdots \\
&= (n+4) + (n+3) + (n+2) + \cdots + (i+5) + T(i) \\
&= \cdots \\
&= (n+4) + (n+3) + (n+2) + \cdots + 6 + T(1) \\
&= (n+4) + (n+3) + (n+2) + \cdots + 6 + 5 \\
&= \sum_{i=1}^{n+4} i - (1+2+3+4) \\
&= \frac{1}{2}(n+5)(n+4) - 10 \\
&= \frac{1}{2}n^2 + \frac{9}{2}n \\
&= \frac{1}{2}n(n+9).
\end{aligned}$$

Any of the last three formulas would be a correct answer.

Problem 4: [12 pts]

Consider the recurrence below defined on $n \geq 1$.

$$T(n) = \begin{cases} 7 & \text{if } n = 1 \\ 25 \cdot T(\frac{n}{5}) + 4n & \text{if } n > 1 \end{cases}$$

(a) Give a closed-form, exact solution for $T(n)$.
Your solution may assume that n is always a power of 5.
You only need to give the solution. You do not need to show how you derived it.

(b) Prove the correctness of your solution by induction.

SOLUTION:

(a) $T(n) = 7n^2 + n(n-1)$.

(b) Let $P(n)$ be "$T(n) = 7n^2 + n(n-1)$".

Base Case:
Let $n = 1$.
Note that $T(1) = 7 = 7 \cdot 1^2 + 1 \cdot (1-1)$, so $P(1)$ is true.

Inductive Case:

Suppose $P(\frac{n}{5})$ is true for $n > 1$. That is, $T(\frac{n}{5}) = 7(\frac{n}{5})^2 + \frac{n}{5}(\frac{n}{5} - 1)$.
By definition,

$$\begin{aligned} T(n) &= 25 \cdot T(\frac{n}{5}) + 4n \\ &= 25 \cdot (7(\frac{n}{5})^2 + \frac{n}{5}(\frac{n}{5} - 1)) + 4n \\ &= 7n^2 + n^2 - 5n + 4n \\ &= 7n^2 + n(n-1) \end{aligned}$$

So, $P(n)$ is true. From the weak principle of mathematical induction, we conclude that the statement is true for $n \geq 1$ where n is a power of 5.

Problem 5: [12 pts]

Alice constructs an RSA key-pair. She first chooses $p = 11, q = 17$ and sets $n = 11 \cdot 17 = 187$. Her secret key is $d = 7$.

Similarly, Bob constructs an RSA key-pair. He first chooses $p = 7, q = 23$ and sets $n = 7 \cdot 23 = 161$. His public key is $(e, n) = (5, 161)$.

(a) What is Alice's public key?

(b) What is Bob's secret key?

(c) Alice wants to send Bob the message $M = 10$. She encrypts the message by the RSA algorithm. What is the value of the encrypted message that Alice sends Bob? Explain how you derived your answer.

SOLUTION:

(a) $T = (p-1)(q-1) = 10 \cdot 16 = 160$
The inverse of 7 in Z_{160} *is 23.*
Thus, Alice's public key is $(e, n) = (23, 187)$.
Note. One way of finding that 23 *is the inverse of* 7 *in* Z_{160} *is by running the extended GCD algorithm on* $7, 160$ *to get*

$$1 = 7 \cdot 23 - 160.$$

(b) $T = (p-1)(q-1) = 6 \cdot 22 = 132$
The inverse of 5 in Z_{132} *is 53.*
Thus, Bob's secret key is $d = 53$.
Note. One way of finding that 53 *is the inverse of* 5 *in* Z_{132} *is by running the extended GCD algorithm on* $5, 132$ *to get*

$$1 = 53 \cdot 5 - 2 \cdot 132.$$

(c) Since Alice wants to send a message to Bob, she uses Bob's public key to encrypt the message. Thus, the encrypted message is $M^5 \bmod 161 = 10^5 \bmod 161 = 19$.

Student ID: _____

Problem 6: [12 pts]

Answer the following questions. For parts (a)-(c), do not forget to justify your answers. For part (d), do not forget to show your calculations.

(a) Is $\left(15^{30} \bmod 31\right) = \left(26^{12} \bmod 13\right)$?

(b) Is $\left(5^{82} \bmod 17\right) = \left(21^{48} \bmod 49\right)$?

(c) Is $\left(7^{75} \bmod 76\right) = \left(6^{73} \bmod 74\right)$?

(d) What is the value of $16^{1161} \bmod 72$?

SOLUTION:

(a) No.
Consider $LHS = 15^{30} \bmod 31$. *Since 31 is a prime number, by Fermat's Little Theorem,* $15^{30} \bmod 31 = 1$.
Consider $RHS = 26^{12} \bmod 13$. *Since 26 is a multiple of 13,* $26^{12} \bmod 13 = 0$.
Thus, $LHS \neq RHS$.

(b) No.
Consider $LHS = 5^{82} \bmod 17$. *Since 17 is a prime number, by Fermat's Little Theorem,* $5^{82} \bmod 17 = 5^{16 \cdot 5 + 2} \bmod 17 = 5^2 \bmod 17 = 8$.
Consider $RHS = 21^{48} \bmod 49$. *Note that*

$$\begin{aligned} 21^{48} \bmod 49 &= 21^{48} - 49q \qquad \textit{where } q \textit{ is a positive integer} \\ &= 21 \cdot 21^{47} - 49q \\ &= 7 \cdot (3 \cdot 21^{47} - 7q) \end{aligned}$$

Thus, $RHS (= 21^{48} \bmod 49)$ *is divisible by 7. However, LHS is not divisible by 7. Thus,* $LHS \neq RHS$.

(c) No.
Consider $LHS = 7^{75} \bmod 76$. *Since any integral power of an odd integer is odd,* 7^{75} *is odd. Note that when we divide an odd number by an even number, the remainder must be odd.*
Consider $RHS = 6^{73} \bmod 74$. *Since any integral power of an even integer is even,* 6^{73} *is even. Note that when we divide an even number by an even number, the remainder must be even.*
Thus, $LHS \neq RHS$.

(d) This can be solved by repeated squaring. Set $I_i = 16^{2^i} \bmod 72$.

$$\begin{aligned}
I_0 &= 16 \\
I_1 &= I_0 \cdot I_0 \bmod 72 = 40 \\
I_2 &= I_1 \cdot I_1 \bmod 72 = 16 \\
I_3 &= I_2 \cdot I_2 \bmod 72 = 40 \\
I_4 &= I_3 \cdot I_3 \bmod 72 = 16 \\
I_5 &= I_4 \cdot I_4 \bmod 72 = 40 \\
I_6 &= I_5 \cdot I_5 \bmod 72 = 16 \\
I_7 &= I_6 \cdot I_6 \bmod 72 = 40 \\
I_8 &= I_7 \cdot I_7 \bmod 72 = 16 \\
I_9 &= I_8 \cdot I_8 \bmod 72 = 40 \\
I_{10} &= I_9 \cdot I_9 \bmod 72 = 16
\end{aligned}$$

Then,

$$\begin{aligned}
16^{1161} \bmod 72 &= 16^{1+8+128+1024} \bmod 72 \\
&= I_0 \cdot I_3 \cdot I_7 \cdot I_{10} \bmod 72 \\
&= 16 \cdot 40 \cdot 40 \cdot 16 \bmod 72 \\
&= 64
\end{aligned}$$

Student ID: _____

Problem 7: [14 pts]
Consider the following two sets of modular equations:

(a)

$$\begin{aligned} x \bmod 21 &= 10 \\ x \bmod 33 &= 30 \end{aligned}$$

(b)

$$\begin{aligned} x \bmod 35 &= 10 \\ x \bmod 33 &= 30 \end{aligned}$$

For each of the two sets of equations answer the following question:

> Does there exist a solution for $x \in Z_{mn}$, where m and n are the divisors of the two modular equations?

Note: in (a), $(m, n) = (21, 33)$; in (b), $(m, n) = (35, 33)$.

For each set, explain why your answer is correct. Furthermore, if your answer is that there is a solution, give a solution.

SOLUTION:

(a) *There is no solution.*
By contradiction, suppose that there was some solution x.
Since $x \bmod 33 = 30$ *we must have, for some integer* q, *that*

$$x = 33q + 30 = 3(11q + 10)$$

so 3 *divides* x, *i.e.,* $x = 3r$ *for some* r.
On the other hand, since $x \bmod 21 = 10$, *we get*

$$x = 21q' + 10$$

for some q', *implying*

$$10 = x - 21q' = 3(r - 7q')$$

so 3 divides 10*! This is false, so there can be no solution to the problem.*
Note that saying that $gcd(21, 33) = 3 \neq 1$ is not *a sufficient answer to this question, since it does not guarantee the non-existence of a solution.*

(b) *Since* $gcd(35, 33) = 1$, *the Chinese Remainder Theorem tells us that there is a unique solution to this problem and further calculation yields* $x = 360$.

Running the Extended GCD algorithm gives

$$1 = 17 \cdot 33 - 16 \cdot 35.$$

Thus the multiplicative inverse of $33 \bmod 35$ *is* 17 *and the multiplicative inverse of* $35 \bmod 33$ *is* $-16 \bmod 33 = 17$ *as well.*

Following the formula in the text we set

$$y = 10 \cdot 17 \cdot 33 + 30 \cdot 17 \cdot 35 = 23460$$

and then set

$$x = y \bmod (1155) = 360$$

to be the answer.

Student ID: _____

Problem 8: [14 pts]

(a) Consider the following quantified statement about elements in some universe U :

$$\neg\forall x \in U\ (\exists y \in U\ (P(x,y) \wedge Q(x,y)\ )\ ) \tag{1}$$

Let $R(x,y) = \neg P(x,y)$ and $S(x,y) = \neg Q(x,y)$.

Express the statement in Equation (1) in terms of $R(x,y)$ and $S(x,y)$. The negation sign ($\neg$) should *not* appear in your statement. Show how you derived your new statement.

(b) For each of the following pair of logical statements, either

(I) prove (using the inference rules discussed in class but *not* a truth table) that the two statements are logically equivalent, or

(II) give a counterexample to show that the statements are not logically equivalent.

A counterexample would be a truth setting of the variables.

(1) (i) $p \Rightarrow (q \Rightarrow r)$
(ii) $(p \wedge q) \Rightarrow r$

(2) (i) $(\neg(p \Rightarrow \neg q)) \Rightarrow (\neg(p \wedge r) \vee s)$
(ii) $(\neg r \Rightarrow p) \Rightarrow ((p \wedge q) \Rightarrow s)$

SOLUTION:

(a) Using the facts

- $\neg\forall x \in U\,(p(x))$ *is equivalent to* $\exists x \in U\,(\neg p(x))$
- $\neg\exists x \in U\,(p(x))$ *is equivalent to* $\forall x \in U\,(\neg p(x))$
- *DeMorgan's laws*

we get

$$\begin{aligned}
& \neg\forall x \in U\ (\exists y \in U\ (P(x,y) \wedge Q(x,y)\ )\ ) \\
= \ & \exists x \in U\ (\neg\exists y \in U\ (P(x,y) \wedge Q(x,y)\ )\ ) \\
= \ & \exists x \in U\ (\forall y \in U\ \neg(P(x,y) \wedge Q(x,y)\ )\ ) \\
= \ & \exists x \in U\ (\forall y \in U\ (\neg P(x,y) \vee \neg Q(x,y)\ )\ ) \\
= \ & \exists x \in U\ (\forall y \in U\ (R(x,y) \vee S(x,y)\ )\ )
\end{aligned}$$

(b) (1) They are equivalent.
Consider

$$\begin{aligned} p \Rightarrow (q \Rightarrow r) &= \neg p \vee (q \Rightarrow r) \\ &= \neg p \vee (\neg q \vee r) \\ &= \neg p \vee \neg q \vee r \end{aligned}$$

Consider

$$\begin{aligned} (p \wedge q) \Rightarrow r &= \neg(p \wedge q) \vee r \\ &= (\neg p \vee \neg q) \vee r \\ &= \neg p \vee \neg q \vee r \end{aligned}$$

Thus, $p \Rightarrow (q \Rightarrow r)$ *is equivalent to* $(p \wedge q) \Rightarrow r$.

(2) They are not equivalent.
When we set $p = T, q = T, r = F, s = F$,
$(\neg(p \Rightarrow \neg q)) \Rightarrow (\neg(p \wedge r) \vee s)$ *becomes true and*
$(\neg r \Rightarrow p) \Rightarrow ((p \wedge q) \Rightarrow s)$ *becomes false.*
Thus, $(\neg(p \Rightarrow \neg q)) \Rightarrow (\neg(p \wedge r) \vee s)$ *is not equivalent to* $(\neg r \Rightarrow p) \Rightarrow ((p \wedge q) \Rightarrow s)$.
(Note: There is only one counter example.)